REMARKS

The application has been amended and is believed to be in condition for allowance.

Claims 1 and 4 have been amended as to form responsive to the claim objection and claim 1 rejection under §112, second paragraph, as indefinite.

Withdrawal of the objection and rejection is solicited.

Claims 1-5, 7, and 9-12 were rejected as obvious over RATAYCZAK 6,259,909 in view of HODGES 5,420,908.

Claims 6 and 8 were rejected as obvious over RATAYCZAK in view of HODGES and further in view of FIELDER 5,995,624.

Applicants respectfully disagree for the reasons outlined below.

RATAYCZAK discloses a process of securing an access to a data processing server from a client site through at least a first communication network, this server comprising means for handling a protocol of authenticating a client site user. This process allows the secure identification of a user by using two individual connections between a first and a second communications device and an access device, in order to transmit a first code and a second code for checking.

RATAYCZAK illustrates on Figures 3 and 5 two realization modes.

The realization mode illustrated on Figure 5 discloses the protocol of authenticating a client site user and comprises a

sequence S51 of receiving and processing identification data ("first code word" column 6, lines 59-64 of RATAYCZAK) from the first communication device C1, and a sequence S52 of transmitting a message ("second code word" column 7, lines 1-5 of RATAYCZAK) from the access device to the second communication device C2 through a second communication network. In a further step S53, the second code word can be transmitted from the second communication device C2 to the first communication device C1, for example, by a read out operation from the first communication device C1 and an input operation at the second communication device C2 (column 7, lines 6-13 of RATAYCZAK). In a further step S54, the second code word is transmitted from the first communication device to access device A and is checked there for correctness (column 7, lines 14-19 of RATAYCZAK).

RATAYCZAK differs from a process according to claim 1 of the application in that RATAYCZAK does not disclose wherein the second code word is a voice message. RATAYCZAK just discloses that the second communication device C2 may be a telephone or a mobile telephone (column 7, line 41 of RATAYCZAK). This is not obvious that the second code word is a voice message. One of ordinary skill in the art would rather transmit the second code word as a text (for example, thanks to a Short Message Service), because it avoids to record voice messages in a data base. Indeed, RATAYCZAK only discloses a read out operation of the second code word (column 5, lines 56-59 of RATAYCZAK) or a

display of the second code word (column 7, lines 8-13 of RATAYCZAK).

Furthermore, RATAYCZAK differs from a process according to claim 1 of the application, in that RATAYCZAK does not disclose wherein the second code word provides to the user means for generating an authentication password intended to be transmitted to the server site. According to RATAYCZAK, the second code word is just transmitted from the second communication device to the first communication device (column 7, lines 6-9 of RATAYCZAK). In a process according to claim 1 of the application, the user can realize an intellectual step: a transmitted message provides to him means for generating an authentication password intended to be transmitted to the server. This intellectual step increases the security level of the process and thus provides an important technical effect.

HODGES discloses a method for use in completing a call from a wireless telephone, comprising the steps of receiving a request at a server (or "mobile switching center") from a communication device (or "wireless telephone"), and transmitting a message (or "challenge") from the server to the communication device.

HODGES does not disclose that the challenge provides to the user means for generating an authentication password, but that this challenge provides to the communication device means for generating an authentication password (or "response")

intended to be transmitted to the server. This has an important technical effect. A process according to HODGES cannot identify the user of the communication device, but just the communication device.

Consider a process resulting from a combination of RATAYCZAK and HODGES. Such process has the same steps that the process illustrated on Figure 5 of RATAYCZAK and previously commented, and could have the further steps of transmitting a challenge from the server to the first and/or the second communication device, the challenge providing to the first and/or second communication device means for generating an authentication password intended to be transmitted to the server, in order to identify the first and/or the second communication device. No message provides to the user means for generating an authentication password. As discussed previously, this generating step provides an important technical effect.

Next, consider a cheater who steals the identification data and the mobile phone of a user. In the case of the process according to RATAYCZAK or resulting from a combination of RATAYCZAK and HODGES, the cheater can transmit the identification data to the server (for example, by Internet), and receive the second code word transmitted to the mobile phone. The cheater can then access to the server. In a process according to the invention, the cheater cannot access to the server, because he does not know how to generate the authentication password.

For these reasons, claim 1 is believed to be non-obvious and thus patentable over RATAYCZAK further in view of HODGES.

Claim 2 comprises the following steps:

"- after establishing a communication with the aforesaid mobile communication equipment, generating a random or pseudo random password;

- sending a voice message comprising the aforesaid random password through the second communication network;

- requesting the user to provide, from the client site through the first communication network, an authentication password derived from the aforesaid random or pseudo random password; and

- authenticating the aforesaid authentication password".

As discussed before, it is not obvious in RATAYCZAK or in a combination of RATAYCZAK and HODGES that the second code word is a voice message. Furthermore, in RATAYCZAK or in a combination of RATAYCZAK and HODGES, the second code word is just transmitted from the second communication device to the first communication device, and thus no authentication password is derived from the second code word. Furthermore, claim 2 is dependent upon claim 1. For all these reasons, claim 2 is believed to be patentable over RATAYCZAK further in view of HODGES.

Claim 3 discloses that the authentication password matches the server generated random or pseudo random password. As discussed before, RATAYCZAK and HODGES do not disclose an authentication password as defined in claim 1. Furthermore, claim 3 is dependent upon claim 2. For these reasons, claim 3 is believed to be patentable over RATAYCZAK further in view of HODGES.

Claim 4 discloses that the authentication password is built from the random or pseudo random password generated by the server and transmitted through the mobile communication equipment, applying a client user known key. RATAYCZAK and HODGES do not disclose a client user known key that allows to build an authentication password from a random or pseudo random password. Furthermore, claim 4 is dependent upon claim 3. For all these reasons, claim 4 is believed patentable over RATAYCZAK further in view of HODGES.

Claim 5 is dependent upon claim 1. For this reason, claim 5 is believed to be patentable over RATAYCZAK further in view of HODGES.

To realize the deciphering and authenticating steps according to claim 7, a server needs to receive three different data from the client site: an encryption key, an authentication password, and a client password. RATAYCZAK and HODGES does not disclose such deciphering and authenticating steps. For example, in a process according to HODGES, the server (or "mobile

switching center") receives only two data from the client site (or "wireless telephone"): a request and a response to a challenge. Furthermore, as discussed before, it is not obvious in RATAYCZAK or in a combination of RATAYCZAK and HODGES that the second code word is a voice message. Claim 7 is dependent upon claim 1. For all these reasons, claim 7 is believed to be patentable over RATAYCZAK further in view of HODGES.

Claim 9 discloses the same subject matter as claim 1, and claim 12 is directed to an application for utilizing the process of claim 1. Claim 10 discloses the same subject matter as claim 2, and claim 11 discloses the same subject matter as claim 7. Thus, claims 9-12 are believed to be patentable over RATAYCZAK further in view of HODGES.

Claim 6 is dependent upon claim 1, and claim 8 is dependent upon claim 7. For these reasons, claims 6 and 8 are believed to be patentable over RATAYCZAK further in view of HODGES and FIELDER.

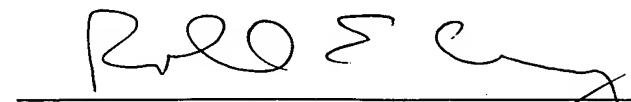
Withdrawal of all of the obviousness rejections is therefore respectfully requested.

The Commissioner is hereby authorized in this, concurrent, and future replies, to charge payment or credit any

overpayment to Deposit Account No. 25-0120 for any additional fees required under 37 C.F.R. § 1.16 or under 37 C.F.R. § 1.17.

Respectfully submitted,

YOUNG & THOMPSON



Roland E. Long, Jr., Reg. No. 41,949
745 South 23rd Street
Arlington, VA 22202
Telephone (703) 521-2297
Telefax (703) 685-0573
(703) 979-4709

REL/lk